IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No. 15128US02

In the Application of:	
	Steve W. Rodgers et al.
U.S. Serial No.:	10/695,008
Filed:	October 28, 2003
For:	SYSTEM AND METHOD FOR SECURING DATA
Examiner:	Daniel L. Hoang
Group Art Unit:	2136
Confirmation No.:	4253
Customer No.:	23446

Certificate of Transmission

I hereby certify that this correspondence is being transmitted via EFS-Web to the United States Patent and Trademark Office on December 14, 2007.

/Michael T. Cruz/
Michael T. Cruz
Reg. No. 44,636

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal was received by the United States Patent and Trademark Office on August 14, 2007 for the above-identified patent application. A Petition for a Two-Month Extension is enclosed, thereby extending the deadline by which to file an Appeal Brief to December 14, 2007.

REAL PARTY IN INTEREST

Broadcom Corporation, a corporation organized under the laws of the state of California and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor.

RELATED APPEALS AND INTERFERENCES

There are currently no appeals or interferences pending regarding related applications.

STATUS OF THE CLAIMS

Claims 1-37 are pending and are being prosecuted in the present application. Claims 1-37 stand rejected. The rejection of claims 1-37 is being appealed.

STATUS OF AMENDMENTS

A Response After Office Action Made Final was filed July 16, 2007. No amendments to the application were made in the Response After Office Action Made Final. In response thereto, an Advisory Action was mailed on August 8, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

Some embodiments according to some aspects of the present invention may provide, for example, a system that protects data as set forth, for example, in claim 1. The system may include, for example, a memory and a processor. The memory may be, for example, a memory in which encrypted data is stored. The processor may be coupled to the memory and may include, for example, a decryptor that decrypts the encrypted data. The decryptor may be adapted to variably bit roll the encrypted data based on at

least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key.

Some embodiments according to some aspects of the present invention may provide, for example, a system that protects data as set forth, for example, in claim 23. The system may include, for example, a memory and a processor. The memory may be, for example, a memory in which encrypted data is stored. The processor may be coupled to the memory and may include, for example, a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline. The decryptor may include, for example, a variable bit roller that variably bit rolls encrypted data based on at least a data address. The decryptor may decrypt a word of the encrypted data in a single cycle.

Some embodiments according to some aspects of the present invention may provide, for example, a system that protects data as set forth, for example, in claim 24. The system may include, for example, a memory and a processor. The memory may be, for example, a memory in which encrypted data is stored. The processor may be coupled to the memory and may include, for example, a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor.

Some embodiments according to some aspects of the present invention may provide, for example, a system that protects data as set forth, for example, in claim 25. The system may include, for example, a memory and a processor. The memory may be, for example, a memory in which encrypted data is stored. The processor may be coupled to the memory and may include, for example, a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle.

Some embodiments according to some aspects of the present invention may provide, for example, a system that protects data as set forth, for example, in claim 26. The system may include, for example, a processor that decrypts encrypted data. The processor may be adapted to variably bit roll encrypted data based on at least a data address and to fixedly bit shuffle the bit-rolled data.

Some embodiments according to some aspects of the present invention may provide, for example, a method that secures processor instructions as set forth, for

example, in claim 30. The method may include, for example, one or more of the following: variably rolling data information based on a first key and an address related to the data information; hard-coded shuffling of the rolled data information; and using one or more keys to process the data information.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1 and 2 are unpatentable under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 4,004,089 to Harold S. Richard et al. ("Richard").

Whether claims 1-37 are unpatentable under 35 U.S.C. § 102(b) as being anticipated by United States Patent Publication No. 2001/0038693 A1 to Frank C. Luyster ("Luyster").

Whether claims 7, 10 and 22 should be objected to under 37 C.F.R. § 1.75(c) as being improper for failing to further limit the subject matter of a previous claim.

ARGUMENT

I. OBJECTIONS WITH RESPECT TO CLAIMS 7, 10 AND 22

A. Claim 10

The Examiner objects to claim 10 under 37 C.F.R. § 1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim. See Office Action Made Final mailed May 14, 2007 ("Office Action Made Final") at page 4. Appellants respectfully request that the Board reverse the objection for at least the reasons as set forth below.

Claim 1 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key".

Claim 10 recites, for example, "wherein the decryptor comprises one or more two-bit adders". Here, the Examiner is assuming that the one or more two-bit adders relate to adding a first key to the bit-shuffled data. Claim 10 does not require such a relationship. Claim 10 merely states that the decryptor comprises one or more two-bit adders. Furthermore, the Examiner is assuming that the first key and the bit-shuffle data must be added in a two-bit adder. There is not such requirement in claim 1. It is respectfully submitted that the Examiner is impermissibly trying to limit the scope of the claims to one or more aspects of one or more of the embodiments as set forth in the specification and/or the drawings.

Appellants respectfully submit that the recited elements as set forth in claim 10 further define the decryptor and that the objection should be reversed.

It is respectfully requested that the Board reverse the objection with respect to claim 10.

B. Claim 22

The Examiner objects to claim 22 under 37 C.F.R. § 1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim. See Office Action Made Final at page 4. From the Examiner's analysis in the Office Action Made Final, it is clear that the Examiner meant claim 22 and not claim 21. Appellants respectfully request that the Board reverse the objection for at least the reasons as set forth below.

Claim 1 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key".

Claim 22 recites, for example, "wherein the decryptor is adapted to receive encrypted data from the memory". Claim 1 recites that the processor is coupled to the memory and that the processor comprises the decryptor. The relationship between the

memory and the decryptor is further defined in claim 22 in that the decryptor is adapted to receive encrypted data from the memory.

Appellants respectfully submit that the recited elements as set forth in claim 22 further define the decryptor and that the objection should be reversed.

It is respectfully requested that the Board reverse the objection with respect to claim 22.

C. Claim 7

The Examiner objects to claim 22 under 37 C.F.R. § 1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim. See Office Action Made Final at page 4. From the Examiner's analysis in the Office Action Made Final, it is clear that the Examiner meant claim 22 and not claim 21. Appellants respectfully request that the Board reverse the objection for at least the reasons as set forth below.

Claim 1 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key".

Claim 7 recites, for example, "wherein the decryptor comprises a fixed bit shuffler". Here, the Examiner is assuming that the fixed bit shuffler relates to fixedly bit shuffle the bit-rolled data. Claim 7 does not require such a relationship. Claim 7 merely states that the decryptor comprises a fixed bit shuffler. It is respectfully submitted that the Examiner is impermissibly trying to limit the scope of the claims to one or more aspects of one or more of the embodiments as set forth in the specification and/or the drawings.

Appellants respectfully submit that the recited elements as set forth in claim 7 further define the decryptor and that the objection should be reversed.

It is respectfully requested that the Board reverse the objection with respect to claim 7.

II. CLAIMS 1 AND 2: RICHARD REJECTION

Claims 1 and 2 stand rejected under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 4,004,089 to Harold S. Richard et al. ("Richard"). Appellants respectfully request that the Board reverse the anticipation rejection based on Richard for at least the reasons as set forth below.

Claim 1 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key".

To maintain the anticipation rejection, each and every element as set forth in claim 1 must be described in Richard.

Claim 1 recites a memory and a processor coupled to the memory. The processor comprises a decryptor.

As set forth in the Office Action Made Final at pages 5 and 6, the Examiner alleges that the memory in claim 1 corresponds to credit card read and write module 30; the processor in claim 1 corresponds to terminal central processing unit (CPU) 10; and the decryptor in claim 1 corresponds to the cryptic device 20.

However, Richard does not describe, as illustrated in FIG. 1, the terminal central processing unit (CPU) 10 comprising the cryptic device 20. In other words, the cryptic device 20 (alleged to be the decryptor) is not part of the terminal central processing unit (CPU) 10 (alleged to be the processor). According, as alleged by the Examiner, Richard does not describe a processor coupled to the memory and comprising a decryptor as set forth in claim 1.

Claim 1 recites "the decryptor being adapted to variably bit roll the encrypted data based on at least a data address".

The Office Action Made Final at pages 5 and 6 alleges that Richard at col. 1, lines 61-65 describes at least these elements as set forth in claim 1. Appellants respectfully disagree.

The cited text does not mention or describe bit rolling at all. Instead, Richard at col. 1, lines 61-65 states "In the present invention the bit outputs from a plurality of linear shift registers are combined in a non-linear sequence generator to provide a bit substitution signal which signal is a long, non-linear pseudo-random sequence bit signal."

In an anticipation rejection in which Richard must describe each and every element as set forth in claim 1, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Richard at col. 1, lines 61-65 does not describe bit rolling. Combining the bit outputs from shift registers does not describe bit rolling. Providing a bit substitution signal which is a long, non-linear pseudo-random sequence bit signal does not describe bit rolling.

Appellants respectfully submit that Richard at col. 1, lines 61-65 appears to relate to an encoding technique. See, e.g., Richard at col. 1, lines 51-57. Thus, it appears that the evidence presented by the Examiner does not appear to describe the *decryptor* being adapted to variably bit roll the encrypted data based on at least a data address.

In fact, although claim 1 recites "the *decryptor* being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key" (italics added). The evidence cited by the Examiner: Richard at col. 1, lines 61-65; col. 2, lines 2-5; col. 1, lines 65-68; and col. 2, lines 5-7 appears to relate to the above-mentioned encoding technique. See, e.g., Richard at col. 1, lines 51-57. It appears that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection under 35 U.S.C. § 102(b).

For at least the above reasons, it is respectfully requested that the rejection under 35 U.S.C. § 102(b) based on Richard be reversed with respect to claim 1 and its rejected dependent claim (i.e., claim 2).

III. CLAIMS 1-4, 7, 9-18, 21 AND 22: LUYSTER REJECTION

Claims 1-4, 7, 9-18, 21 and 22 stand rejected under 35 U.S.C. § 102(b) as being anticipated by United States Patent Publication No. 2001/0038693 A1 to Frank C. Luyster

("Luyster"). Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 1 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key".

To maintain the anticipation rejection, each and every element as set forth in claim 1 must be described in Luyster.

Claim 1 recites "the decryptor being adapted to variably bit roll the encrypted data based on at least a data address".

In the Office Action Made Final at page 7, the Examiner alleges that Luyster at paragraph [0095] describes at least these elements as set forth in claim 1. In particular, the Examiner recites "a bit-moving function capable of rotating bits (or of otherwise moving bits into different positions) of one-to-one round segments by predetermined numbers of bits" as allegedly describing the above elements as set forth in claim 1.

It appears from the Examiner's recitation from paragraph [0095] of Luyster that the bit-moving function does not variably bit roll, but instead rotates bits by predetermined number of bits.

It also appears from the Examiner's recitation that the alleged variable bit roll (i.e., the rotating bits by a predetermined amount) is not based on a data address as set forth in claim 1.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claim 1, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe a decryptor being adapted to variably bit roll the encrypted data based on at least a data address.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 1

and its rejected dependent claims (i.e., claims 2-4, 7, 9-18, 21 and 22).

Claim 1 recites "the decryptor being adapted ... to fixedly bit shuffle the bit-rolled data".

In the Office Action Made Final at page 7, the Examiner alleges that Luyster at paragraph [0095] describes at least these elements as set forth in claim 1. In particular, the Examiner recites "a linear combination function which provides new round segments using a round operator generally from a first algebraic group to combine two different round segments; and a nonlinear function which affects a round segment based on a value which depends on bits from another round segment, where both round segments are different round segments from the same one-to-one round segment set" as allegedly describing at least the above elements as set forth in claim 1.

Appellants respectfully submit that the cited text does not describe a decryptor adapted to fixedly bit shuffle the bit-rolled data. In fact, the above-cited text does not mention fixedly bit shuffling at all and certainly does not describe fixedly bit shuffling the bit-rolled data as set forth in claim 1.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claim 1, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe a decryptor being adapted to variably bit roll the encrypted data based on at least a data address.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 1 and its rejected dependent claims (i.e., claims 2-4, 7, 9-18, 21 and 22).

IV. CLAIMS 5 AND 6

Claims 5 and 6 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claims 5 and 6 depend from claim 1. Accordingly, the arguments made with respect to claim 1 are also made with respect to claims 5 and 6.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claims 5 and 6.

In addition, claims 5 and 6 recite subject matter that is not described in Luyster.

Claim 5 recites "wherein the bit roller comprises a plurality of multiplexers".

Claim 6 recites "wherein each multiplexer comprises a multiplexer selection input, wherein multiplexer selection bits are input at the multiplexer selection input, and wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key".

In the Office Action Made Final at pages 8 and 9, the Examiner alleges that Luyster at paragraphs [125] and [138] describes at least the above elements as set forth in claims 5 and 6.

In particular, the Examiner alleges that a bit roller comprising a plurality of multiplexers is described in Luyster at paragraph [125] in the following: "Linear Operators are drawn from the list of all operators computed as part of the instruction set of a typical microprocessor which have two inputs, and examples of linear operators include addition, subtraction, SIMD addition, SIMD subtraction, and bit-wise exclusive-or, where such SIMD (Single Instruction Multiple Data) operations include either addition or subtraction executed in parallel (e.g., MMX-style addition of 2 segments of 32-bits each from two 64-bit registers). Linear Operators are restricted to those operators computed as part of the instruction set of a typical microprocessor which have the properties that (1) given two inputs with an equal probability of containing 0's and 1's, the output of the operator contains generally an equal probability of 0's and 1's, and (2) given that either input is constant, the output is a one-to-one function of the other input.".

Appellants respectfully submit that multiplexers are no where mentioned in the above recitation from Luyster. In fact, multiplexer is not mentioned anywhere in Luyster.

Perhaps the Examiner thought that claims 5 and 6 recited multipliers instead of multiplexers. Respectfully, it is difficult to discern the Examiner's allegation.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claims 5 and 6, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe "wherein the bit roller comprises a plurality of multiplexers" as set forth in claim 5 and does not describe "wherein each multiplexer comprises a multiplexer selection input, wherein multiplexer selection bits are input at the multiplexer selection input, and wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key" as set forth in claim 6.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claims 5 and 6.

V. CLAIM 8

Claim 8 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 8 depends from claim 1. Accordingly, the arguments made with respect to claim 1 are also made with respect to claim 8.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 8.

In addition, claim 8 recites subject matter that is not described in Luyster.

Claim 8 recites "wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler".

In the Office Action Made Final at page 9, the Examiner alleges that Luyster at paragraph [124] describes at least these elements as set forth in claim 8. In fact, the cited

text on which the Examiner relies to maintain the anticipation rejection is as follows: "In the present example, each block half is computed in one 64-bit register."

It is respectfully submitted that just because something is "computed" in a "register" does not mean that the "register" is a hard-coded bit shuffler and, in particular, a fixed, hard-coded bit shuffler. In fact, the Examiner alleges in the Office Action Made Final that the register is part of a CPU. Thus, allowing for the possibility, that the computation is a software computation.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claim 8, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe "wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler" as set forth in claim 8.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 8.

VI. CLAIM 19

Claim 19 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 19 depends from claim 1. Accordingly, the arguments made with respect to claim 1 are also made with respect to claim 19.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 19.

In addition, claim 19 recites subject matter that is not described in Luyster.

Claim 19 recites "wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor".

In the Office Action Made Final at page 12, the Examiner alleges that Luyster at paragraph [227] describes at least these elements as set forth in claim 19. In fact, the

cited text on which the Examiner relies to maintain the anticipation rejection is as follows: "Fixed rotations by non-zero numbers of bits are a subset of the possible bit-permutations, and unlike most bit-permutations, have the advantage of generally being executed in one clock cycle on a microprocessor."

It is respectfully submitted that does not even mention a decryptor that does not add enough gate delays to exceed a clock cycle budget of the processor. Just one round in the block decryption of Luyster would include a lot more than the above-mentioned fixed rotation. A quick glance at Luyster at FIG. 3 illustrates that there are many, many other components in a single round.

In addition, it is also noted that decryption would take a plurality of *rounds* according to the description of Luyster. This is further evidence that a decryptor according to Luyster would probably add enough gate delays to exceed a clock cycle budget of the processor.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claim 19, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe "wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor" as set forth in claim 19.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 19.

VII. CLAIM 20

Claim 20 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 20 depends from claim 1. Accordingly, the arguments made with respect to claim 1 are also made with respect to claim 20.

For at least the above reasons, it is respectfully requested that the Board reverse the

anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 20.

In addition, claim 20 recites subject matter that is not described in Luyster.

Claim 20 recites "wherein the decryptor decrypts a word of the encrypted data in a single cycle".

In the Office Action Made Final at page 12, the Examiner alleges that Luyster at paragraph [97] describes at least these elements as set forth in claim 20. In fact, the cited text on which the Examiner relies to maintain the anticipation rejection is as follows: "Embodiments of this Feistel or near-Feistel approach generally modify each of the primary round segments in each round of calculation in the same way, typically using operations which modify all the bits of the large primary round segments in single linear operations."

It is respectfully submitted that does not even mention decrypting a word of the encrypted data in a single cycle. Even if the single linear operations somehow represented a single cycle (which is not described in the cited text), decryption may include other operations not mentioned in the cited text which may thus exceed a single cycle. There is not enough information here. The above description may be focusing only on one small part of a larger decryption process. Thus, even if the single linear operations represented a single cycle (which is not described in the cited text), it does not guarantee that decrypting a word of the encrypted data occurs in a single cycle.

It is also noted that decryption would take a plurality of *rounds* according to the description of Luyster. This is further evidence that decrypting a word of the encrypted data probably does not occur in a single cycle.

In an anticipation rejection in which Luyster must describe each and every element as set forth in claim 20, Appellants respectfully submit that the Examiner has not met the burden of proof necessary to maintain an anticipation rejection. Luyster at Examiner's citation does not describe "wherein the decryptor decrypts a word of the encrypted data in a single cycle" as set forth in claim 20.

For at least the above reasons, it is respectfully requested that the Board reverse the

anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 20.

VIII. CLAIM 23

Claim 23 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 23 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline, wherein decryptor comprises a variable bit roller that variably bit rolls encrypted data based on at least a data address, and wherein the decryptor decrypts a word of the encrypted data in a single cycle."

Since claim 23 recites "wherein decryptor comprises a variable bit roller that variably bit rolls encrypted data based on at least a data address", arguments similar to the arguments made with respect to claim 1 are made here for claim 23 for similar elements.

Since claim 23 recites "wherein the decryptor decrypts a word of the encrypted data in a single cycle" which is the same or similar to the elements as set forth in claim 20, arguments that the same or similar to the arguments made with respect to claim 20 are made here with respect to claim 23 for the same or similar elements.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 23.

IX. CLAIM 24

Claim 24 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 24 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor".

Since claim 24 recites "a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor", arguments similar to the arguments made with respect to claim 19 are made here for claim 24 for similar elements.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 24.

X. CLAIM 25

Claim 25 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 25 recites "a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle".

Since claim 25 recites "a decryptor that ... decrypts a word of the encrypted data in a single cycle", arguments similar to the arguments made with respect to claim 20 are made here for claim 25 for similar elements.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 25.

XI. CLAIMS 26-29

Claim 26 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 26 recites "a processor that decrypts encrypted data, the processor being adapted to variably bit roll encrypted data based on at least a data address and to fixedly bit shuffle the bit-rolled data".

Since claim 26 elements that are the same or similar to elements recited in claim 1, arguments similar to the arguments made with respect to claim 1 are made here for claim 26 for similar elements.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 26 and its rejected dependent claims (i.e., claims 27 and 28).

XII. CLAIMS 30-37

Claim 30 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Luyster. Appellants respectfully request that the Board reverse the anticipation rejection based on Luyster for at least the reasons as set forth below.

Claim 30 recites "variably rolling data information based on a first key and an address related to the data information; and hard-coded shuffling of the rolled data information; using one or more keys to process the data information".

Since claim 30 elements that are the same or similar to elements recited in claim 1, arguments similar to the arguments made with respect to claim 1 are made here for claim 26 for similar elements.

Since claim 30 elements that are the same or similar to elements recited in claim 8, arguments similar to the arguments made with respect to claim 8 are made here for claim 26 for similar elements.

For at least the above reasons, it is respectfully requested that the Board reverse the anticipation rejection based on 35 U.S.C. § 102(b) based on Luyster with respect to claim 30 and its rejected dependent claims (i.e., claims 31-37).

XIII. CONCLUSION

For the foregoing reasons, it is believed that claims 1-37 are patentable over the alleged prior art of record. Reversal of the Examiner's rejection of claims 1-37 is therefore respectfully requested, thereby placing claims 1-37 in condition for allowance. Accordingly, issuance of a patent on the application is therefore respectfully requested.

The Commissioner is hereby authorized to charge any additional fees, to charge any fee deficiencies or to credit any overpayments to the deposit account of McAndrews, Held & Malloy, Account No. 13-0017.

Dated: December 14, 2007

Respectfully submitted,

/Michael T. Cruz/
Michael T. Cruz
Registration No. 44,636

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775-8100

CLAIMS APPENDIX

The following claims are involved in this appeal:

1. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data based on at least a data address, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key.

2. The system according to claim 1, wherein the decryptor is adapted to perform a single pipeline stage decryption.

3. The system according to claim 1, wherein the decryptor comprises a bit roller that rotates data in one or more roll regions of the incoming data based on the data address related to the received encrypted data and a key related to the first key.

4. The system according to claim 3, wherein the key comprises a shifted version of the first key.

5. The system according to claim 3, wherein the bit roller comprises a plurality of multiplexers.

6. The system according to claim 5,

wherein each multiplexer comprises a multiplexer selection input,

wherein multiplexer selection bits are input at the multiplexer selection input, and

wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key.

7. The system according to claim 1, wherein the decryptor comprises a fixed bit shuffler.

8. The system according to claim 7, wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler.

9. The system according to claim 7, wherein the fixed bit shuffler does not add a gate delay to the decryptor.

10. The system according to claim 1, wherein the decryptor comprises one or more two-bit adders.

11. The system according to claim 10, wherein each two-bit adder comprises three exclusive OR (XOR) gates and an AND gate.

12. The system according to claim 1, wherein the decryptor comprises an XOR block.

13. The system according to claim 12, wherein the XOR block comprises one or more XOR gates.

14. The system according to claim 13, wherein each XOR gate comprises a first input and a second input, the first input receiving a bit of the second key, the second input receiving a bit of the added data.

15. The system according to claim 1, wherein the first key is a shifted version of a key.

16. The system according to claim 15, wherein an amount of shift in the first key is based on the data address related to the received encrypted data.

17. The system according to claim 15, wherein the first key is generated substantially in parallel with the decrypting of the encrypted data.

18. The system according to claim 1, wherein the decryptor does not add a latency to a processor pipeline.

19. The system according to claim 1, wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor.

20. The system according to claim 1, wherein the decryptor decrypts a word of the encrypted data in a single cycle.

21. The system according to claim 1, wherein the word comprises a 64-bit word.

22. The system according to claim 1, wherein the decryptor is adapted to receive encrypted data from the memory.

23. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline,

wherein decryptor comprises a variable bit roller that variably bit rolls encrypted data based on at least a data address, and

wherein the decryptor decrypts a word of the encrypted data in a single cycle.

24. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor.

25. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle.

26. A system for securing data, comprising:

a processor that decrypts encrypted data, the processor being adapted to variably bit roll encrypted data based on at least a data address and to fixedly bit shuffle the bit-rolled data.

27. The system according to claim 26, wherein the processor is adapted to perform a single pipeline stage decryption.

28. A system according to claim 26, wherein the processor is adapted to add a first key to the bit-shuffled data and to process the added data with a second key.

29. The system according to claim 26, wherein the processor is adapted to decrypt the encrypted data without adding a latency to a processor pipeline.

30. A method for securing processor instructions, comprising:

variably rolling data information based on a first key and an address related to the data information; and

hard-coded shuffling of the rolled data information;

using one or more keys to process the data information.

31. The method according to claim 30, wherein the rolling, the shuffling and the using are part of a single pipeline stage decryption.

32. The method according to claim 30, wherein using one or more keys to process the data information comprises adding the hard-coded data information and a shifted version of the first key.

33. The method according to claim 32, wherein using one or more keys to process the data information comprises processing the added data information with a second key using exclusive OR (XOR) gates.

34. The method according to claim 33, wherein the first key is not a function of the second key.

35. The method according to claim 30, wherein the data information comprises encrypted data information.

36. The method according to claim 30,

wherein the encrypted data information is stored in a memory, and

wherein the stored data information is accessed by a processor.

37. The method according to claim 30, wherein the rolling comprises rotating bits within one or more rolling regions of the data information.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.